Security
Section 4

Chapter 8

P2 Known- plaintext attack
→ 7- letters Known
→ For all un-Known possible 26!
→ For 7 Letters Known

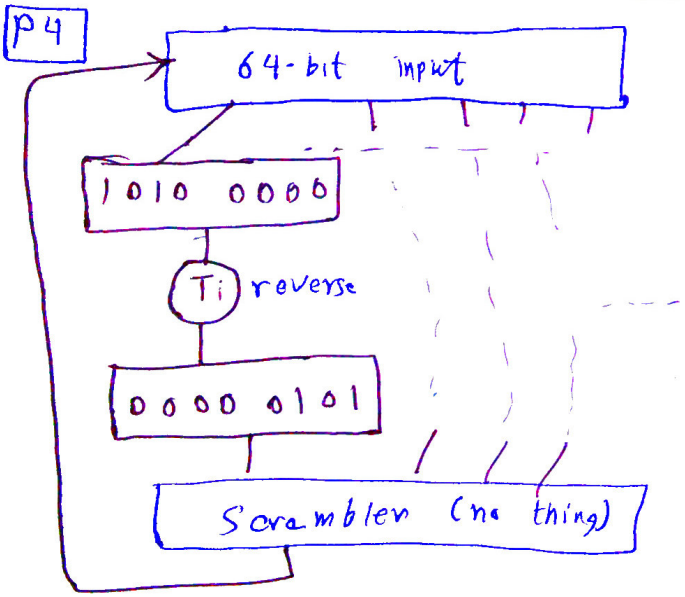
$$(26-7)! = 19!$$

We reduce possiblity by

$$26! - 19! = 10^9$$

P3 Yes, It's possible to Know the key of cipher 1,2 ((shift))

P4



(a) result after n= 3
[0000 0101][0000 0101]----

(b) the input
[1010 0000]---- 1010 0001
the result
[0000 0101]---- 1000 0101

(c) Scramblen also reverse order

الى بيده الجوسين هو الجزء المتكرر

Step 1
before Scramblen
[0000 0101] ---- 1000 0101
after
1010 0001 --- [1010 0000]

Step 2
before Scramblen
1000 0101 --- [0000 0101]
after
[1010 0000]--- 1010 0001

Step 3
before
[0000 0101] --- 1000 0101
after
1010 0001 --- [1010 0000]

P6 (a) 100 100 100
011 011 011

(b) She can Know the pattern

(c) m(1) = 100
m(2) = 100
m(3) = 100

→ IV = C(0) = 111
→ C(1) = Ks(C(0) ⊕ m(1))
= Ks (011) = 100
→ C(2) = Ks (c(1) ⊕ m(2))
= Ks (000) = 110
→ C(3) = Ks (C(2) ⊕ m(3))
= Ks (010) = 101

m= 100 100 100 C = 100 110 101

P7 $p=3 \quad q=11$

① $n = p \cdot q = 33$

$z = (p-1)(q-1) = 20$

② $e < n$ — e → has no common factor with z

20 → 20 10 5 4 2

$e = 9$ → we choose this

$e * d \ \% \ z = 1$

$d = ??$

$9 * d \ \% \ 20 = 1$

$9 * 9 \ \% \ 20 = 1$

$d = 9$

③ $C = m^e \ \% \ n$

'd' → $m = 4$ → $C = 4^9 \ \% \ 33$

'o' → $m = 15$ → $C = 15^9 \ \% \ 33$

'9' → $m = 7$ → $C = 7^9 \ \% \ 33$

④ $m = c^d \ \% \ n$

P9 $T_A = 9^{S_A} \ \% \ P$

$T_B = 9^{S_B} \ \% \ P$

$S = T_B^{S_A} \ \% \ P$

$S' = T_A^{S_B} \ \% \ P$ → Prove that they are equal

$S = [9^{S_B} \ \% \ P]^{S_A} \ \% \ P$

$= 9^{S_A S_B} \ \% \ P$

$= [9^{S_A} \ \% \ P]^{S_B} \ \% \ P$

$= T_A^{S_B} \ \% \ P = S'$